A PROJECT REPORT

ON

VULNERABLE UNIVERSITY

SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR OF

BACHELOR OF TECHNOLOGY
COMPUTER ENGINEERING

SUBMITTED BY

ABHISHEK BIRDAWADE	**BCOA03**
SRUSHTI DESHPANDE	**BCOB93**
VAIBHAV WAGH	**BCOB111**

UNDER THE GUIDANCE OF

MS. GAYATRI BEDRE

DEPARTMENT OF COMPUTER ENGINEERING

G. H. RAISONI COLLEGE OF ENGINEERING AND MANAGEMENT

(An Autonomous Institute affiliated to SPPU)

WAGHOLI, PUNE –
412207

SAVITRIBAI PHULE PUNE UNIVERSITY

2022 - 2023

CERTIFICATE

This is to certify that the project report entitled

VULNERABLE UNIVERSITY

Submitted by

ABHISHEK BIRDAWADE	**BCOA03**
SRUSHTI DESHPANDE	**BCOB93**
VAIBHAV WAGH	**BCOB111**

Are bonafide students of this institute and the work has been carried out by them under the supervision of **Ms. Gayatri Bedre** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Technology** (Computer Engineering).

Ms. Gayatri Bedre		**Dr. Simran Khiani**
Internal Guide	External	Hod – Computer Engineering

Dr. R. D. Kharadkar
Director

Place: Pune

Date:

ACKNOWLEDGEMENT

We are profoundly grateful to **Ms. Gayatri Bedre** for her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion.

We would like to express deepest appreciation towards **Dr. R. D. Karadkar**, Director, G. H. Raisoni College of Engineering and Management, Pune, Dr. Simran Khiani, Head of Department, Computer Engineering and **Mrs. Mansi Bhonsle**, Project Coordinator whose invaluable guidance supported us in completing this project.

At last, we must express our sincere heartfelt gratitude to all the staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

ABHISHEK BIRDAWADE ……………...
SRUSHTI DESHPANDE ……………...
VAIBHAV WAGH ……………..

ABSTRACT

In recent years, cybersecurity has become increasingly crucial due to the rise of cyber-attacks and the complexity of cybercriminals. As technology advances, the need for skilled security testers and practitioners who can identify and fix vulnerabilities without violating cyber laws has become paramount. Application vulnerabilities have emerged as one of the most significant concerns, as they can lead to severe issues if exploited by malicious actors. To meet the expanding demands of the cybersecurity field, there is a growing need for effective ways to learn and test security skills. Intentionally vulnerable web applications have emerged as a valuable tool in this regard, providing a simulated environment for security professionals to practice offensive and defensive operations on their local systems.

Intentionally vulnerable web applications allow security professionals to enhance their skills in web application security testing. By working with these applications, professionals can gain hands-on experience in identifying and fixing technical and non-technical bugs and vulnerabilities. This practical training enables them to develop a deep understanding of web security threats and equips them with the expertise needed to implement robust security measures. These web applications simulate real-world web environments, providing security professionals with a platform to prepare for real-world opportunities. By practicing on intentionally vulnerable applications, professionals can become well-versed in the tactics and techniques used by cybercriminals. This familiarity enables them to proactively protect organizations from potential cyber-attacks.

One of the key benefits of using intentionally vulnerable web applications is the opportunity to stay up-to-date with the latest security threats. As new vulnerabilities and attack vectors emerge, security professionals can explore and understand them within a controlled environment. This knowledge equips them to anticipate and respond effectively to evolving cyber threats. In addition to technical skills, vulnerable web applications also help professionals develop non-technical abilities. This includes critical thinking, problem-solving, and the ability to assess risk and prioritize security measures. By engaging with these applications, security practitioners gain a holistic approach to cybersecurity, ensuring the confidentiality, integrity, and availability of critical data and systems.

The hands-on experience provided by vulnerable web applications is crucial for security professionals to build their confidence and competence. Working in a simulated environment allows them to make mistakes and learn from them without compromising real-world systems. This iterative learning process strengthens their abilities and prepares them for the challenges they may face in their careers. Intentionally vulnerable web applications also play a vital role in fostering a collaborative and proactive security culture within organizations. By involving security professionals in offensive and defensive operations, these applications encourage knowledge sharing, collaboration, and teamwork. This collaborative approach enhances the overall security posture of organizations by ensuring that a diverse range of perspectives and expertise is applied to threat mitigation.

Vulnerable web applications can be utilized in various contexts, such as individual training, team exercises, or even as part of capture-the-flag competitions. These applications offer flexibility in terms of customization, allowing organizations to tailor the environment to their specific needs and objectives. This versatility makes them valuable tools for both educational and professional purposes.

Keywords: Cybersecurity, Vulnerable University, Ethical hacking, Penetration testing, Cyber threats, Cybersecurity professionals, Cybersecurity students, IT security managers, Freelance ethical hackers, Learning and testing, Open-source application, GitHub, Docker file.

INDEX

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

Synopsis

With the increasing prevalence of cyber-attacks, the importance of cybersecurity has never been more evident. Among the biggest concerns for cybersecurity are application vulnerabilities, which can result in serious issues. To combat these vulnerabilities, skilled security testers and practitioners are needed who can identify and fix them without breaking any laws. One effective way of acquiring these skills is by using intentionally vulnerable web applications that provide a simulated environment for security professionals to practice offensive and defensive operations on their local system.

Intentionally vulnerable web applications offer a platform for security professionals to practice their skills in web application security testing. These applications simulate real-world web environments, giving professionals a realistic experience in handling cyber threats. By identifying and fixing technical and non-technical bugs and vulnerabilities, security professionals can better prepare themselves for real-world opportunities and help organizations protect against cyber-attacks. With these web applications, professionals can enhance their knowledge of the latest security threats and implement robust security measures to counter them.

The benefits of using intentionally vulnerable web applications are numerous. These applications provide security professionals with a safe environment to practice and develop their skills without putting any real systems at risk. Furthermore, these applications offer a way to test different scenarios and tactics that may not be feasible in a real-world environment. Additionally, these applications can help professionals gain a better understanding of the impact of cyber-attacks on business operations and the importance of cybersecurity.

In conclusion, intentionally vulnerable web applications provide an effective way for security professionals to enhance their skills in web application security testing. By utilizing these applications, professionals can gain a better understanding of the latest security threats and implement robust security measures to counter them. These web applications offer a safe environment to practice and develop skills while providing a realistic experience of handling cyber threats. With the increasing demand for cybersecurity professionals, the use of intentionally vulnerable web applications is expected to rise in the future.

CHAPTER 2

Technical Keywords

2.1 Area of Project:

The area of project for the above topic is focused on the development and implementation of intentionally vulnerable web applications to enhance the skills of security professionals in web application security testing, including identifying and fixing technical and non-technical bugs and vulnerabilities, and preparing them for real-world opportunities to help organizations protect against cyber-attacks. This project aims to create a simulated environment that replicates real-world web environments and provides security professionals with a platform to practice offensive and defensive operations on their local systems, enabling them to gain an in-depth understanding of the latest security threats and implement robust security measures to counter them.

2.2 Technical Keywords

1. K. Computing Milieu
   - (a) K.6 Security and Privacy
     - i. K.6.1 Authentication
     - ii. K.6.2 Access controls
     - iii. K.6.3 Integrity and confidentiality
     - iv. K.6.4 Security and privacy policies
     - v. K.6.5 Security and protection mechanisms
     - vi. K.6.6 Human factors and usability
2. D. Software
   - (a) D.2 Software Engineering
     - i. D.2.10 Design
     - ii. D.2.13 Reusable software
     - iii. D.2.9 Management
   - (b) D.4 Operating Systems
     - i. D.4.6 Security and Protection

CHAPTER 3

Introduction

3.1. Project Idea:

The project idea for intentionally vulnerable web applications is focused on creating a simulated environment that replicates real-world web environments and provides security professionals with a platform to practice offensive and defensive operations on their local systems. The primary objective of this project is to enhance the skills of security professionals in web application security testing, including identifying and fixing technical and non-technical bugs and vulnerabilities, and preparing them for real-world opportunities to help organizations protect against cyber-attacks.

One of the key aspects of this project is to develop intentionally vulnerable web applications that contain a range of vulnerabilities, including technical and non-technical bugs. These web applications will simulate real-world web environments and provide security professionals with a platform to practice their skills in identifying and fixing vulnerabilities without violating cyber laws. The project will also focus on creating a comprehensive learning environment that includes detailed documentation and training materials to help security professionals understand the latest security threats and implement robust security measures to counter them.

Another important aspect of this project is to provide security professionals with the tools and resources they need to test their skills in a safe and controlled environment. This includes developing a virtual machine environment that can be easily configured to replicate different web application environments and provide security professionals with a platform to practice their skills in a controlled setting. The project will also focus on creating a community of security professionals who can share their experiences and insights to help others learn and grow in the field of web application security testing.

3.2. Motivation of the Project:

The motivation behind the project of intentionally vulnerable web applications is to address the growing need for skilled security testers and practitioners who can identify and fix vulnerabilities in web applications without violating cyber laws. With the rise of cyber-attacks and the sophistication of cyber criminals, organizations need to take proactive steps to protect their web applications from potential security breaches.

One of the biggest challenges that organizations face is the shortage of skilled security professionals who can identify and fix vulnerabilities in web applications. While there is a growing demand for security professionals in this field, many organizations struggle to find individuals with the necessary skills and experience. This project aims to address this challenge by providing a platform for security professionals to practice and enhance their skills in web application security testing.

Another motivation behind this project is to create a safe and controlled environment for security professionals to test their skills. By creating intentionally vulnerable web applications, security professionals can engage in offensive and defensive operations on their own local systems without violating cyber laws. This allows them to gain practical experience in identifying and fixing vulnerabilities in web applications and prepare for real-world opportunities.

Finally, this project is motivated by the need to create a community of security professionals who can share their experiences and insights to help others learn and grow in the field of web application security testing. By providing a platform for security professionals to connect and collaborate, this project can play a critical role in building a strong and vibrant community of experts who can work together to protect organizations against cyber-attacks.

3.3. Literature Survey:

1. "A Survey of Web Application Vulnerabilities" by N. B. Saleh and A. A. Ali: This paper provides an overview of the most common web application vulnerabilities, including injection flaws, broken authentication and session management, cross-site scripting, and others. The paper also discusses the impact of these vulnerabilities and provides recommendations for mitigating

them.

2. "Vulnerable Web Applications for Hands-on Learning and Testing" by J. C. Torres et al.: This paper proposes the use of intentionally vulnerable web applications as a tool for hands-on learning and testing of web application security. The paper describes the development of several vulnerable web applications and their use in training and testing environments.

3. "Web Application Security: Threats, Countermeasures, and Pitfalls" by V. M. Campos and P. G. B. da Silva: This paper provides an overview of web application security threats, including server-side attacks, client-side attacks, and authentication and session management issues. The paper also discusses countermeasures for these threats and highlights common pitfalls in web application security.

4. "A Framework for Developing Intentionally Vulnerable Web Applications" by N. F. M. Noordin et al.: This paper proposes a framework for developing intentionally vulnerable web applications. The framework includes a set of requirements, design principles, and implementation guidelines for creating web applications with intentional vulnerabilities.

CHAPTER 4

Problem Definition & Scope

4.1 Problem Statement:

As cyber-attacks and digital thefts become more frequent, cybersecurity has become a major concern. However, there is a significant challenge in finding accessible and user-friendly platforms for security testing and learning that do not violate cyber laws. The lack of such platforms presents a major obstacle for individuals seeking to improve their cybersecurity skills. To address this challenge, the Vulnerable University project aims to provide a secure and user-friendly platform for cybersecurity testing and learning, accessible to users of all skill levels. This will help to create a safer and more secure digital landscape for everyone.

4.1.1 Goal & Objectives

Goal and Objectives:

- To identify the threats in the system.
- To measure the potential vulnerabilities of the system.
- To help in detecting every possible security risk in the system.
- To help developers in fixing the security problems through coding.

4.1.2 Statement of Scope

The scope of the project of intentionally vulnerable web applications is to create a platform for security professionals to practice and enhance their skills in web application security testing. The project aims to develop a set of intentionally vulnerable web applications that simulate real-world web environments and provide a safe and controlled environment for security professionals to test their skills. The scope of the project includes the following:

- Developing intentionally vulnerable web applications: The project will involve the development of a set of intentionally vulnerable web applications that simulate real-world web environments. These web applications will include various types of vulnerabilities, such as injection flaws, broken authentication and session management, cross-site scripting, and others.

- Providing a safe and controlled environment: The project will ensure that the intentionally vulnerable web applications are safe and controlled, and do not violate any cyber laws. This will involve implementing appropriate security measures to protect the web applications from potential security breaches.
- Creating a community of security professionals: The project aims to create a community of security professionals who can connect and collaborate to share their experiences and insights. This will involve developing a platform for security professionals to interact with each other and share their knowledge and expertise.
- Enhancing web application security testing skills: The project aims to enhance the skills of security professionals in web application security testing. This will involve providing resources and tools to help security professionals identify and fix vulnerabilities in web applications.

The scope of the project is limited to the development of intentionally vulnerable web applications and providing a safe and controlled environment for security professionals to test their skills. The project does not aim to provide comprehensive training in web application security testing, but rather to complement existing training programs and provide a platform for security professionals to practice and enhance their skills.

4.2 Major Constraints:

One major constraint in the project of intentionally vulnerable web applications is the need to ensure that the web applications do not violate any cyber laws and do not pose a threat to the security of users or organizations. This will require the project team to conduct extensive testing and implement appropriate security measures to protect the web applications from potential security breaches. Another constraint is the availability of resources, including funding, skilled personnel, and technology infrastructure, which may limit the scope and scale of the project. Additionally, the project team will need to ensure that the intentionally vulnerable web applications are designed in a way that is both realistic and challenging, while also being safe and controlled. Finally, the project team will need to consider the ethical implications of creating intentionally vulnerable web applications and ensure that they are used for educational and training purposes.

4.3 Methodologies of Problem solving and efficiency issues:

To develop the intentionally vulnerable web applications, the project team will adopt a number of methodologies for problem-solving and enhancing efficiency. These methodologies include:

- Agile development: The project team will adopt an agile development methodology, which involves iterative and incremental development. This approach will enable the team to quickly respond to changes in requirements and feedback from users and stakeholders.
- Risk-based testing: The project team will adopt a risk-based testing approach, which involves identifying the most critical areas of the web applications and focusing testing efforts on those areas. This approach will enable the team to identify and fix vulnerabilities more efficiently.
- Automated testing: The project team will use automated testing tools to enhance the efficiency of testing. This will include using tools such as static analysis, dynamic analysis, and fuzz testing to identify and fix vulnerabilities.
- Continuous integration and delivery: The project team will adopt a continuous integration and delivery approach, which involves automating the build and deployment process. This approach will enable the team to quickly deploy new features and fixes to the intentionally vulnerable web applications.

4.4 Outcome:

The outcome of developing intentionally vulnerable web applications is to provide a platform for security professionals to enhance their skills in web application security testing. By practicing offensive and defensive operations in a simulated real-world web environment, security professionals can identify and fix technical and non-technical bugs and vulnerabilities, without violating cyber laws. The intentionally vulnerable web applications can also help organizations protect against cyber-attacks by training their security professionals to better prepare for real-world opportunities. Overall, the outcome of this project is to enhance the skills and capabilities of security professionals, ultimately leading to a safer and more secure digital world.

4.5 Applications:

Here are some potential applications of intentionally vulnerable web applications:

- Training and education: Intentionally vulnerable web applications can be used to train and educate security professionals on web application security testing.
- Penetration testing: Organizations can use intentionally vulnerable web applications to conduct penetration testing to identify and fix vulnerabilities in their own web applications.
- Security assessment: Intentionally vulnerable web applications can be used to assess the security posture of organizations by identifying potential vulnerabilities in their web applications.
- Research: Intentionally vulnerable web applications can be used for research purposes to study the impact of cyber-attacks and the effectiveness of different security measures.
- Certification and accreditation: Intentionally vulnerable web applications can be used to certify and accredit security professionals and organizations in web application security testing.

4.6 Hardware Resources Required:

Sr. No.	Parameter	Minimum Requirement	Justification
1	HDD	1 TB	Remark Required
2	RAM	4/8 GB	Remark Required

4.7 Software Resource Required:

Platform:

- Operating System: Linux, Windows
- Web Browser: Firefox, Chrome, etc

CHAPTER 5

Project Plan

5.1 Project Estimates:

The estimates for developing intentionally vulnerable web applications will depend on various factors such as the complexity of the web applications, the number of vulnerabilities to be integrated, the development methodology adopted, the testing tools utilized, and the size of the project team. As a rough estimate, it may take several months to develop a set of intentionally vulnerable web applications, along with the necessary documentation and testing. The cost of development may also vary depending on the location and expertise of the development team. Additionally, ongoing maintenance and updates may be required to ensure the web applications remain relevant and effective in identifying and fixing vulnerabilities. Overall, the development of Vulnerable University requires significant time, resources, and expertise, but can have a significant impact on enhancing the skills and capabilities of security professionals in web application security testing.

5.1.1 Reconciled Estimates

Cost and time estimates for developing vulnerable university can vary widely depending on the specific project requirements, such as the complexity of the application, the number of vulnerabilities to be integrated, and the development team's size and expertise.

It is also important to note that ongoing maintenance and updates may be required to ensure the application remains relevant and effective, which can add additional costs and time requirements.

5.1.2 Project Resources

Developing vulnerable university requires a variety of resources, including:

- Skilled development team: A team of skilled developers is required to design and implement the intentionally vulnerable web application.
- Testing tools: Appropriate testing tools are necessary to identify vulnerabilities

in the web application.

- Development environment: A development environment with appropriate software and hardware resources is needed for the development team to build the web application.
- Documentation and training materials: Documentation and training materials must be created to help users understand how to use and navigate the intentionally vulnerable web application.
- Budget and funding: Adequate budget and funding are necessary to support the development and ongoing maintenance of the intentionally vulnerable web application.
- Time and project management: Proper time and project management is crucial to ensure that the development team can complete the project on time and within budget.

5.2 Risk Management:

As developing intentionally vulnerable web applications involves identifying and intentionally integrating security vulnerabilities, there is a risk that the application could be exploited by malicious actors. Additionally, the complexity of the web application and the potential for unforeseen vulnerabilities to be introduced can make it difficult to guarantee its security.

This presents a risk management challenge, as it is important to balance the benefits of creating intentionally vulnerable web applications for training and testing purposes with the potential security risks they pose. One way to mitigate these risks is to conduct a thorough NP Hard analysis to identify potential vulnerabilities and their potential impact. This can help inform the development process and prioritize security measures to minimize the risk of exploitation. Additionally, it is important to ensure that the intentionally vulnerable web applications are only used in controlled and secure environments to limit the potential impact of any security breaches.

5.2.1 Risk Identification:

Identifying potential risks is an important part of developing vulnerable university. Some of the potential risks that need to be identified and mitigated include:

Security risks: The vulnerable university itself can be a potential security risk, as it may be exploited by malicious actors. Additionally, the development process can introduce unforeseen vulnerabilities that need to be addressed.

Legal risks: Intentionally creating and distributing a vulnerable web application can potentially violate laws and regulations related to cybercrime and hacking. It is important to ensure that the application is only used for lawful purposes.

Operational risks: The development process for vulnerable university can be complex and time-consuming, with potential delays and issues that can impact the project's timeline and budget.

Ethical risks: There are ethical considerations to be taken into account when developing vulnerable university. These include ensuring that the application is used for legitimate purposes and that its use does not harm others.

By identifying and mitigating these potential risks, the development team can ensure that the vulnerable university is safe, ethical, and effective for its intended purpose.

5.2.2 Risk Analysis:

Risk analysis table for the development of vulnerable university:

Risk	Probability	Impact	Mitigation Strategy
Security vulnerabilities introduced during development	High	High	Conduct regular security audits and penetration testing throughout the development process to identify and address vulnerabilities. Follow industry-standard security protocols and best practices.
Legal violations related to cybercrime or hacking	Medium	High	Ensure that the intentionally vulnerable web application is only used for lawful purposes and does not violate any laws or regulations. Provide clear guidelines and disclaimers for users.
Delay in project timeline due to complexity of development process	Medium	Medium	Plan project timeline carefully, with built-in contingencies for unforeseen delays. Prioritize project milestones and allocate

			resources effectively.
Misuse of intentionally vulnerable web application for unethical purposes	Low	High	Establish clear usage guidelines and codes of conduct for users. Monitor usage and take action against any misuse or unethical behavior.

Table 5.1: Risk Table

Probability	Value	Description
High	Probability of occurrence is	> 75%
Medium	Probability of occurrence is	26 – 75%
Low	Probability of occurrence is	< 25%

Table 5.2: Risk Probability definitions

5.3 Project Schedule:

5.3.1 Project Task Set:

1. Conduct initial research on existing intentionally vulnerable web applications and identify gaps and opportunities for improvement.
2. Define project scope and objectives, and develop a project plan with clear timelines, milestones, and deliverables.
3. Conduct a risk analysis and develop a risk mitigation strategy.
4. Develop a design and architecture for the intentionally vulnerable web application, including user interface, functionality, and security features.
5. Develop a database schema and integrate with the web application.
6. Implement front-end and back-end development, including user authentication and authorization, data input and validation, and API development.
7. Conduct regular testing and debugging throughout the development process, including unit testing, integration testing, and user acceptance testing.
8. Implement security features and conduct regular security audits and penetration testing to identify and address vulnerabilities.

9. Develop documentation and training materials for users, including guidelines for ethical use and security best practices.
10. Launch the intentionally vulnerable web application and monitor usage and performance, addressing any issues or concerns that arise.

CHAPTER 6

Software Requirement Specification

6.1 Introduction:

6.1.1 Purpose & Scope of Document:

The Vulnerable University application can be used by developers, security auditors, and penetration testers to practice and enhance their skills in web application security testing. The article concludes that the Vulnerable University application is an invaluable resource for anyone looking to learn and develop their skills in web application security testing.

6.1.2 Overview of Responsibilities:

Designing and implementing software solutions: Developers are responsible for creating software that meets the requirements and specifications of the project. Testing and debugging software: Developers are responsible for ensuring that the software functions correctly and meets the requirements.

Maintaining and updating software: Developers are responsible for maintaining and updating the software they create. This involves fixing bugs, adding new features, and making improvements to the software over time.

6.2 Usage Scenario:

The vulnerable university system can be used for various scenarios related to web application security testing. Here are some examples:

- Practice for Security Professionals: Security professionals can use the vulnerable university system to practice and improve their web application security testing skills. They can identify the vulnerabilities and try to exploit them, and then work on fixing them.
- Training for Students: Universities and other educational institutions can use the system as a training tool for students who are studying web application security. It can provide a practical environment for students to learn and practice their skills.
- Assessment for Security Audits: Organizations can use the vulnerable university

system as a part of their security audit process. They can test their own web application security by using the system and identify the vulnerabilities and risks associated with their applications.

- Research and Development: Researchers and developers can use the system to study the impact of various web application vulnerabilities and explore new ways to secure web applications.

6.2.1 User Profiles:

The profiles of all user categories are described here: -

1. Education: - The project can be used for educating and training individuals, including students, professionals, and cybersecurity enthusiasts, on cybersecurity vulnerabilities and how to identify and mitigate them.
2. Testing: - The project can be used as a testing ground for conducting penetration testing, vulnerability assessments, and other security tests.

6.2.2 Use Cases:

Sr No.	Use Case	Description	Actors	Assumptions
1	Login	User enters their username and password to access the system	Student, Faculty, Staff	User has a valid account and the correct credentials
2	View Grades	User can view their own grades for their enrolled courses	User	User is enrolled in at least one course and the course has been graded
3	Access Learnin g Module	User can access the learning module to learn new bugs	User	User is accessing the vulnerable university on their local system.

Table 6.1: Use Cases

6.2.3 Use Case View

- User – Security Professionals, Testers, Developers
- Application
- Types of Vulnerabilities
- Reports
- Severity

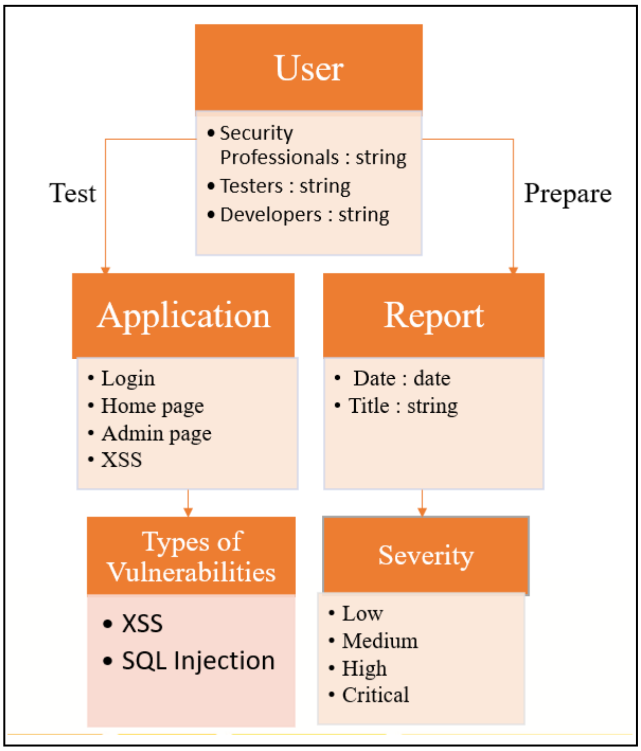


Figure 6.1: Use case diagram

CHAPTER 7

Detailed Design Document

7.1 Introduction:

The Vulnerable University application was intentionally designed with various vulnerabilities to provide a safe and controlled environment for users to learn and practice web application security testing. The design included the creation of multiple web pages, forms, and databases containing vulnerabilities such as XSS, SQL injection, and authentication bypass.

The application is available to anyone interested in learning and practicing web application security testing. Usage data is collected to improve the application and identify any areas that may require additional security measures. The application does not collect any personal data from its users.

7.2 Architectural Design:

The collected usage data is analysed to identify trends and patterns in user behaviour, which is used to improve the application and ensure that it continues to provide a safe and effective learning environment for individuals interested in web application security testing.

The application ensures confidentiality, integrity, and availability of data by providing appropriate security measures. Authentication and authorization mechanisms are used to provide authorized access to users and ensure non-repudiation, ensuring that none of the parties involved in a transaction can dispute subsequent involvement.

7.3 Data Design:

Overall, the methodology used to design and implement the Vulnerable University application ensures that it is an effective tool for individuals to learn and practice web application security testing in a safe and controlled environment.

7.3.1 Internal Software Data Structure:

Data The internal software data structure for a project depends on the specific requirements and functionality of the project. In general, a software data structure refers to the way that data is organized and stored in memory by a computer program.

7.3.2 Global Data Structure:

Data global data structure refers to a data structure that is accessible and can be modified from anywhere within a program or system. It is a data structure that is defined in a global scope, meaning it can be accessed by any function or module within the program.

7.3.3 Temporary Data Structure:

A temporary data structure, as the name suggests, is a data structure that is created and used temporarily for a specific task or purpose.

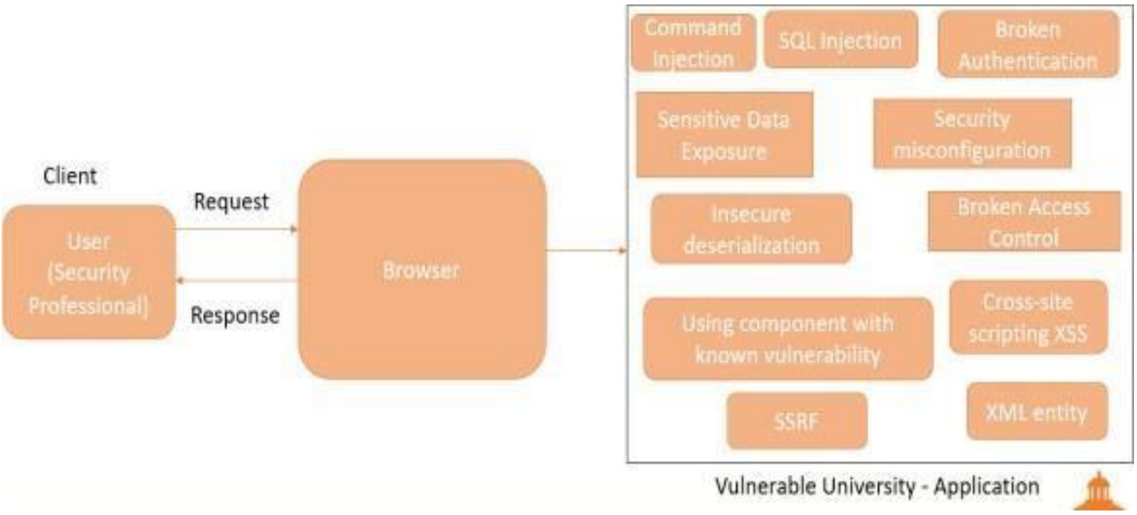


Figure 7.1: Vulnerable University Architecture diagram

7.3.4 Database Description:

Database is a collection of structured data that is organized and stored in a computer system. It is designed to facilitate efficient and secure storage, retrieval, and manipulation of data for various purposes, such as record-keeping, analysis, and decision-making. In this project we had used SQL database.

7.3.5 Class Diagram:

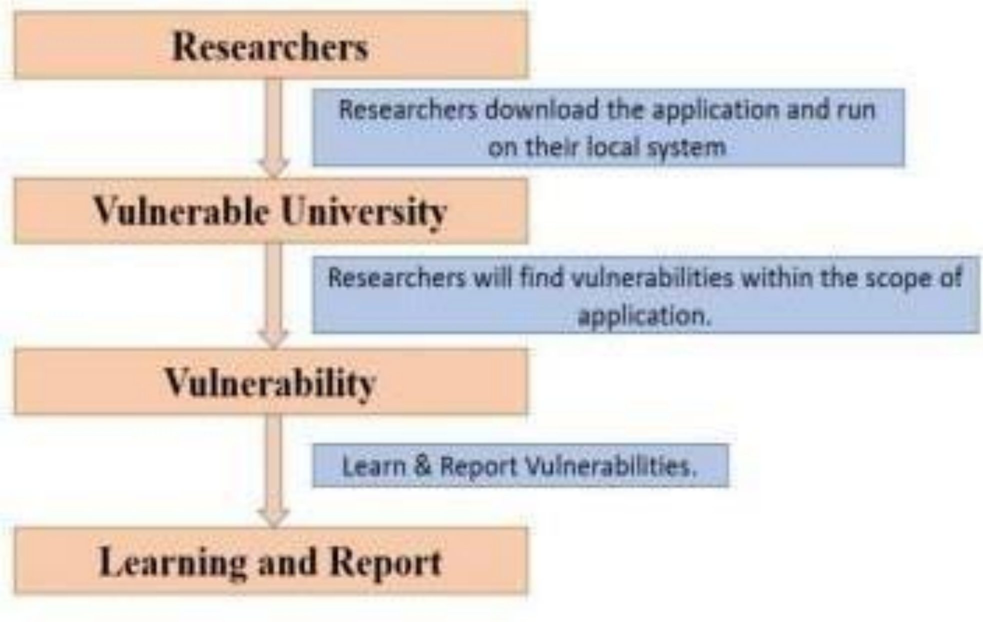

Researchers
Researchers download the application and run on their local system
Vulnerable University
Researchers will find vulnerabilities within the scope of application.
Vulnerability
Learn & Report Vulnerabilities.
Learning and Report

Figure 7.2: Class Diagram

CHAPTER 8

Project Implementation

8.1 Introduction:

The implementation of an intentionally vulnerable web application involves the development of a web application with known security vulnerabilities. This project is essential in the field of cybersecurity as it provides a platform for security professionals to practice and enhance their skills in web application security testing. By utilizing intentionally vulnerable web applications, security professionals can better prepare for real-world opportunities and help organizations protect against cyber-attacks.

The implementation of the intentionally vulnerable web application involves the development of a front-end and back-end of the web application, including designing and coding the website, creating databases, and ensuring that the website is responsive and user-friendly. Security features are then implemented to prevent cyber-attacks and data breaches, with potential vulnerabilities identified and addressed. Quality assurance testing is conducted to ensure that the web application meets requirements and functions correctly. Finally, documentation and training materials are created for users and other stakeholders.

The implementation of an intentionally vulnerable web application is a crucial step in improving cybersecurity in organizations. This project provides an opportunity for security professionals to enhance their skills in web application security testing, helping to identify and address potential vulnerabilities before they can be exploited by cybercriminals.

8.2 Tools and Technologies Used:

The development of a vulnerable university involves the use of various tools and technologies to create a functional and secure web application. Below are some of the commonly used tools and technologies for this project:

- Programming Languages: HTML, CSS, JavaScript, Python, and SQL are commonly used programming languages for web application development.
- Web Application Frameworks: Popular web application frameworks include Laravel, Django and NodeJS. These frameworks provide a structure for developing web applications, making it easier to develop and maintain web applications.
- Databases: Databases such as MySQL, PostgreSQL, and MongoDB are commonly used for storing data in web applications.
- Web Servers: Web servers like Apache and Nginx are used to host web applications and provide access to them over the internet.
- Security Tools: Security tools such as OWASP ZAP, Burp Suite, and Metasploit can be used to identify and address vulnerabilities in web applications.
- Version Control Systems: Git and SVN are commonly used version control systems for web application development.
- Integrated Development Environments (IDEs): IDEs like Visual Studio Code, Eclipse provides a development environment for creating and testing web applications.

8.3 Methodologies / Algorithms Details:

The methodology for developing an intentionally vulnerable web application involves several steps, as outlined below:

- Planning: In this phase, the project goals and objectives are defined, along with the project scope, timeline, and resource requirements. This phase also involves identifying the stakeholders, defining the user requirements, and creating a project plan.
- Design: In this phase, the functional and technical requirements are translated into a design specification, which includes the architecture, user interface, database schema, and security features of the web application. This phase also involves identifying the tools and technologies to be used and creating a prototype.
- Development: In this phase, the web application is developed using the chosen programming languages, frameworks, and tools. This involves coding the functionality, creating the database schema, and testing the application for bugs

and vulnerabilities.

- Testing: In this phase, the application is tested using various security testing tools to identify and address any vulnerabilities. This phase includes both functional and security testing.
- Deployment: In this phase, the application is deployed to a production environment or a staging environment for further testing. This phase also involves configuring the web server and database, setting up security measures, and monitoring the performance of the application.
- Maintenance: In this phase, the application is monitored and maintained to ensure that it continues to function properly and is secure against new threats. This phase includes regular updates and bug fixes, as well as ongoing security testing and vulnerability assessments.

8.4 Verification and Validation for Acceptance:

Verification and validation can be achieved by testing the vulnerable web applications thoroughly using various techniques such as black-box testing, penetration testing, and vulnerability scanning. The testing should cover both technical and non-technical vulnerabilities, including input validation errors, session management issues, and SQL injection attacks.

CHAPTER 9

Software Testing

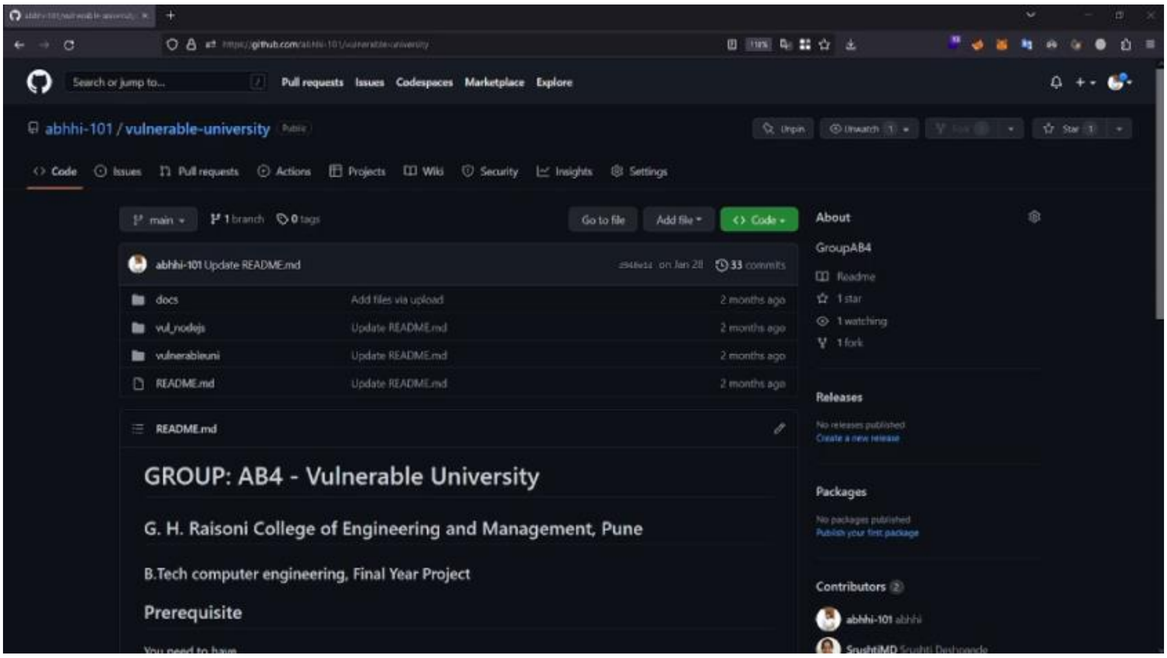
9.1 Types of Testing Used:

- Black-box testing: This type of testing involves testing the application from an external perspective without any knowledge of the internal workings of the application. Testers attempt to break the application by testing inputs and outputs, and observing the behavior of the application.
- White-box testing: This type of testing involves testing the application from an internal perspective, with knowledge of the internal workings of the application. Testers attempt to break the application by testing specific components or modules of the application.
- Penetration testing: This type of testing involves testing the application's security by attempting to exploit vulnerabilities or weaknesses in the application. Testers attempt to gain unauthorized access to the system, steal sensitive information, or disrupt the normal functioning of the application.
- Vulnerability scanning: This type of testing involves scanning the application for known vulnerabilities or weaknesses. Testers use specialized tools to scan the application and identify vulnerabilities such as unsecured ports, weak passwords, and outdated software.
- User acceptance testing: This type of testing involves testing the application with actual users to ensure that the application meets their needs and expectations. Testers observe how users interact with the application and gather feedback to improve the user experience.

CHAPTER 10

Results and Discussion

10.1 Screenshots:



abhhi-101 Update README.md on Jan 28 33 commits

docs	Add files via upload	2 months ago
vul_nodejs	Update README.md	2 months ago
vulnerableuni	Update README.md	2 months ago
README.md	Update README.md	2 months ago

README.md

GROUP: AB4 - Vulnerable University

G. H. Raisoni College of Engineering and Management, Pune

B.Tech computer engineering, Final Year Project

Prerequisite

You need to have

About

GroupAB4

Readme

1 star

1 watching

1 fork

Releases

No releases published

Create a new release

Packages

No packages published

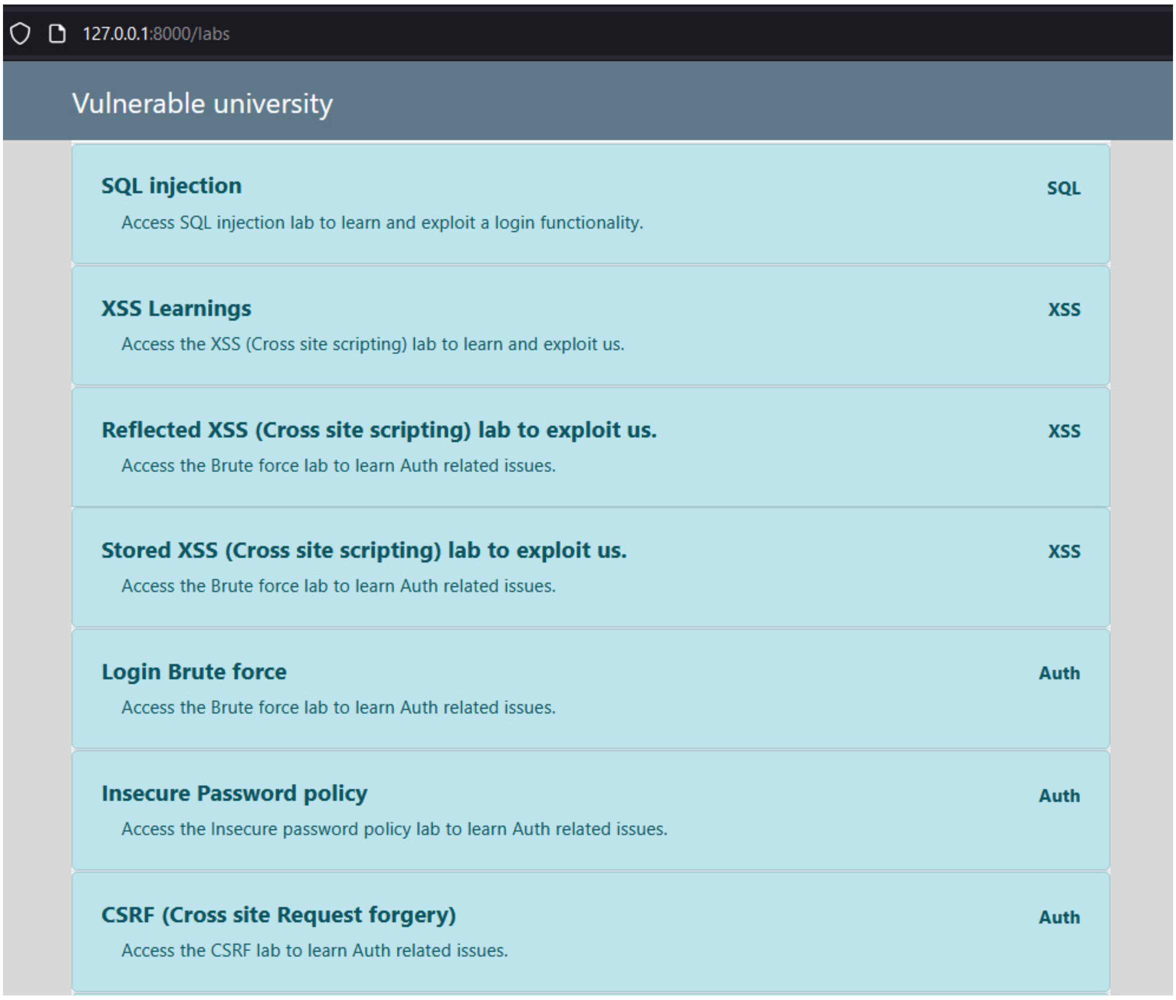
Publish your first package

Contributors 2

abhhi-101 abhhi

SrushtiMD Srushti Deshpande

10.2 Outputs:



127.0.0.1:8000/labs

Vulnerable university

SQL injection SQL

Access SQL injection lab to learn and exploit a login functionality.

XSS Learnings XSS

Access the XSS (Cross site scripting) lab to learn and exploit us.

Reflected XSS (Cross site scripting) lab to exploit us. XSS

Access the Brute force lab to learn Auth related issues.

Stored XSS (Cross site scripting) lab to exploit us. XSS

Access the Brute force lab to learn Auth related issues.

Login Brute force Auth

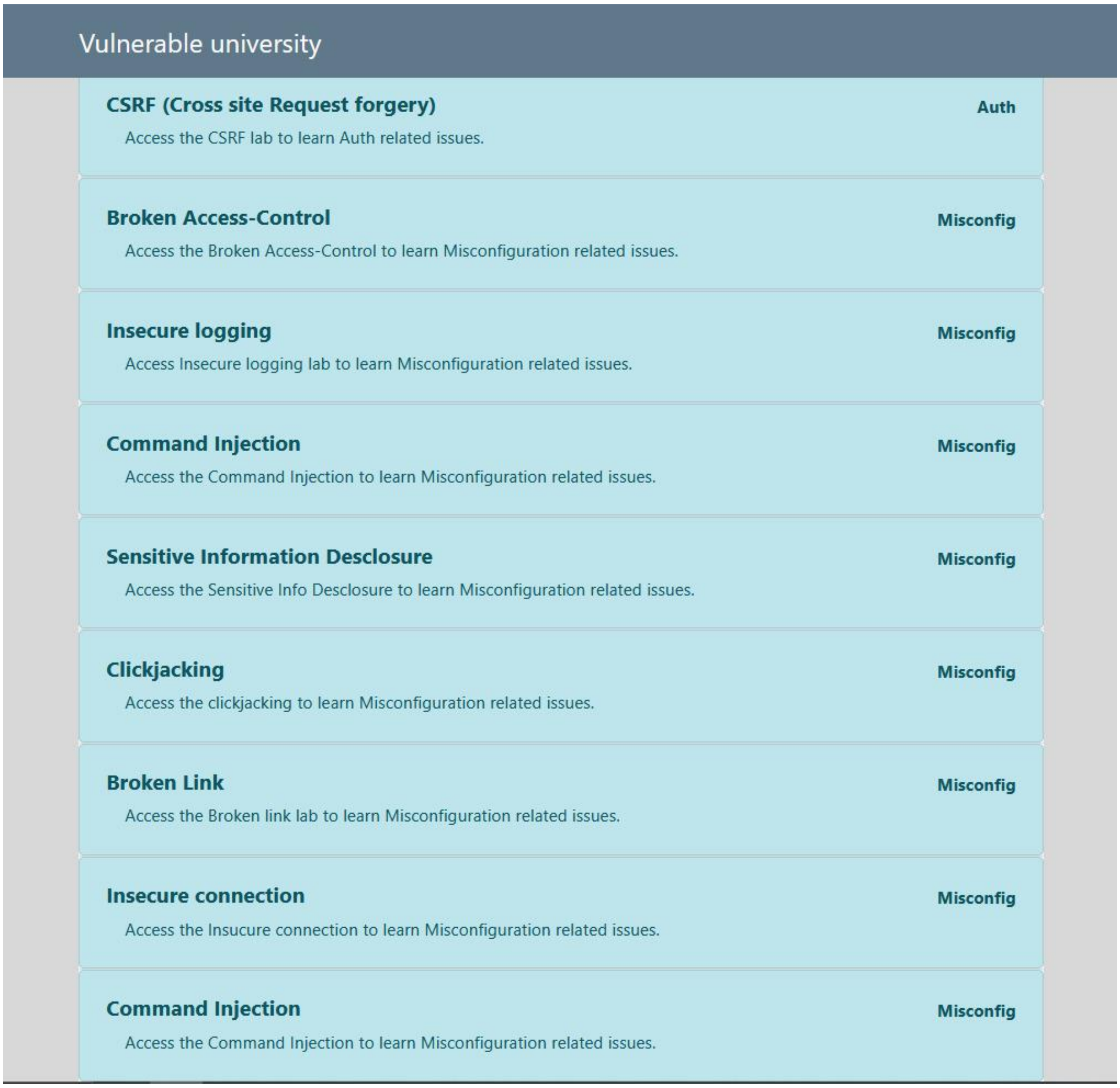
Access the Brute force lab to learn Auth related issues.

Insecure Password policy Auth

Access the Insecure password policy lab to learn Auth related issues.

CSRF (Cross site Request forgery) Auth

Access the CSRF lab to learn Auth related issues.



Vulnerable university

CSRF (Cross site Request forgery) Auth

Access the CSRF lab to learn Auth related issues.

Broken Access-Control Misconfig

Access the Broken Access-Control to learn Misconfiguration related issues.

Insecure logging Misconfig

Access Insecure logging lab to learn Misconfiguration related issues.

Command Injection Misconfig

Access the Command Injection to learn Misconfiguration related issues.

Sensitive Information Desclosure Misconfig

Access the Sensitive Info Desclosure to learn Misconfiguration related issues.

Clickjacking Misconfig

Access the clickjacking to learn Misconfiguration related issues.

Broken Link Misconfig

Access the Broken link lab to learn Misconfiguration related issues.

Insecure connection Misconfig

Access the Insucure connection to learn Misconfiguration related issues.

Command Injection Misconfig

Access the Command Injection to learn Misconfiguration related issues.

CHAPTER 11

Deployment and Maintenance

11.1 Installation and un-installation:

11.1.1 Project Requirements:

To install this project, you need some software's pre-installed on your Operating System as follows:

a. `git` command line tool - https://git-scm.com/book/en/v2/Getting-Started-Installing-Git

b. Docker-Desktop - https://www.docker.com/products/docker-desktop/Installation steps

c. Browser –

- Firefox - https://www.mozilla.org/en-US/firefox/new/
- Chrome - https://www.google.com/chrome/
- Brave - https://try.bravesoftware.com/ujw151
- Tor - https://www.torproject.org/download/

11.1.2 Installation on Windows:

Follow the below step:-

1. Open Windows command-prompt
2. Clone the repository locally using git

```
git clone https://github.com/abhhi-101/vulnerable-university.git
```

3. Move to the newly cloned repository directory.

```
- cd vulnerable-university
```

4. We have added 2 Vulnerable Applications:
   a. Using Python's framework Django called vul_django
   b. Similarly, using JavaScript's framework Nodejs called vul_nodejs

5. To install vul_django
   a. Change current working directory to vul_django using,
      ```
      - cd vul_django
      ```
   b. Now you can start the application using Docker using,
      ```
      - docker-compose up -d
      ```
6. To Stop the application.
   ```
   - docker ps
   - docker stop <process_id>
   ```
7. Follow further instructions in README.md file.
8. Similarly, to start vul_nodejs application, follow step 5,6,7

11.1.3 Installation on Linux:

Follow the below step:-

1. Open Linux command-prompt
2. Clone the repository locally using git
   ```
   git clone https://github.com/abhhi-101/vulnerable-university.git
   ```

3. Move to the newly cloned repository directory.

```
- cd vulnerable-university
```

4. We have added 2 Vulnerable Applications:

   1.Using Python's framework Django called vul_django

   2. Similarly, using JavaScript's framework Nodejs called vul_nodejs

5. To install vul_django

   1. Change current working directory to vul_django using,

   ```
   - cd vul_django
   ```

   2. Now you can start the application using Docker using,

   ```
   - docker-compose up -d
   ```

6. To Stop the application.

```
- docker ps
- docker stop <process_id>
```

7. Follow further instructions in README.md file.

8. Similarly, to start vul_nodejs application, follow step 5,6,7

11.2 User Help:

Build Docker Image and Run:-

1. Build the docker image from DockerFile using,

   ```
   docker build –f Dockerfile –t vul_django
   ```

2. Run the docker image!

   ```
   docker run  --rm –p 8000:8000 vul_django:latest
   ```

3. Browse to http://127.0.0.1:8000 or http://0.0.0.0:8000

CHAPTER 12

Conclusion and Future Scope

12.1 Conclusion:

Vulnerable University application is a valuable platform for individuals to learn and practice web application security testing in a safe environment. The application has been well-received by professionals in various fields and has helped users improve their web application security testing skills. Its positive impact on increasing awareness and the importance of web application security makes it an essential tool for anyone interested in the field. Continued education and training in cyber security is crucial, and the Vulnerable University application provides a means to improve skills and contribute to a more secure digital future.

In summary, the Vulnerable University application is a valuable platform for anyone interested in improving their web application security testing skills. The application's positive impact on the awareness and importance of web application security and the growth of skilled security testers and practitioners in the field makes it an essential tool for building a more secure digital environment. With the continued use and development of the application, individuals can enhance their skills and contribute to the overall security and protection of organizations and individuals in the digital age.

12.2 Future Scope:

- Providing students with a virtual lab environment where they can experiment with various tools and techniques in a safe and controlled manner.
- Offering guidance and tutorials on different hacking techniques and concepts, such as social engineering, network scanning, and exploitation.
- Offering guidance and tutorials on different hacking techniques and concepts, such as social engineering, network scanning, and exploitation.

Appendix A

References

[1] Adam Doupe and Marco Cova and Giovanni Vigna. Why johnny can’t pentest: An analysis of black-box web vulnerability scanners. In DIMVA 2010, 2010.

[2] N. Ayewah, D. Hovemeyer, J. D. Morgenthaler, J. Penix, and W. Pugh. Experiences using static analysis to find bugs. IEEE Software, 25:22– 29, 2008. Special issue on software development tools, September/October (25:5).

[3] R. Bachmann and A. D. Brucker. Developing secure software: A holistic approach to security testing. Datenschutz und Datensicherheit (DuD), 38(4):257–261, apr 2014.

[4] P. Ammann and J. Offutt. Introduction to Software Testing. Cambridge University Press, Cambridge, UK, 2008.

[5] J. Grossman, R. Hansen, P. Petkov, and A. Rager. Cross Site Scripting Attacks: XSS Exploits and Defense. Syngress, 2007.

[6] M. Anisetti, C. Ardagna, and E. Damiani. A low-cost security certification scheme for evolving services. In Web Services (ICWS), 2012 IEEE 19th International Conference on, pages 122–129, June 2012.

[7] B. Arkin, S. Stender, and G. McGraw. Software penetration testing. Security & Privacy, IEEE, 3(1):84–87, 2005.

[8] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell. State of the art: Automated black-box web application vulnerability testing. In Security and Privacy (SP), 2010 IEEE Symposium on, pages 332–345. IEEE, 2010.

[9] A. D. Brucker, L. Br¨ugger, and B. Wolff. Formal firewall conformance testing: An application of test and proof techniques. Software Testing, Verification & Reliability (STVR), 25(1):34–71, 2015.

Appendix B

Project Planner

There are various project management tools available in the market, and the selection of a tool will depend on the specific needs of your project. Some popular project management tools are:

- Trello: Trello is a user-friendly project management tool that uses boards, lists, and cards to manage tasks and projects. It allows users to create and assign tasks, set deadlines, and track progress. Trello is a great option for small teams or individuals who need a simple yet effective project management solution.
- Asana: Asana is a comprehensive project management tool that offers a wide range of features, including task management, team collaboration, time tracking, and project planning. It is a great option for larger teams or projects that require a more robust solution.
- Jira: Jira is a popular project management tool that is widely used in software development projects. It offers a range of features such as agile boards, issue tracking, and project reporting. Jira is a great option for software development teams that need a powerful project management solution.
- Basecamp: Basecamp is a project management tool that offers a range of features such as task management, team collaboration, and project tracking. It is a great option for teams that need a simple and intuitive project management solution.
- Monday.com: Monday.com is a visual project management tool that uses boards and timelines to manage projects. It offers a range of features such as task management, team collaboration, and project reporting. Monday.com is a great option for teams that need a visually appealing and easy-to-use project management solution.

Appendix C

Paper Published Summary

a) Conference Paper

Paper Title: Vulnerable University

Name of the Conference/Journal where paper submitted: International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023).

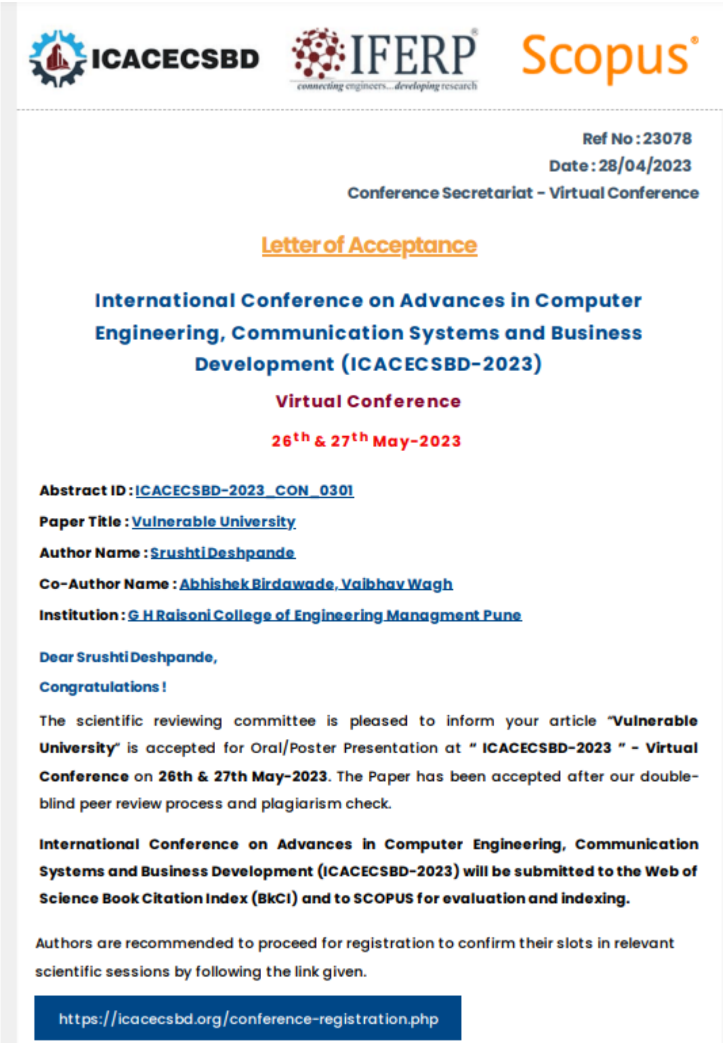
Paper accepted/rejected: Paper Accepted

Conference Date: 26th May 2023

Ref No.: 23078

Paper Id: ICACECSBD-2023_CON_0301

Acceptance Letter (Conference Paper) -



ICACECSBD IFERP Scopus

Ref No : 23078
Date : 28/04/2023
Conference Secretariat - Virtual Conference

Letter of Acceptance

International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023)

Virtual Conference

26th & 27th May-2023

Abstract ID : ICACECSBD-2023_CON_0301

Paper Title : Vulnerable University

Author Name : Srushti Deshpande

Co-Author Name : Abhishek Birdawade, Vaibhav Wagh

Institution : G H Raisoni College of Engineering Managment Pune

Dear Srushti Deshpande,

Congratulations !

The scientific reviewing committee is pleased to inform your article "**Vulnerable University**" is accepted for Oral/Poster Presentation at " **ICACECSBD-2023** " - **Virtual Conference** on **26th & 27th May-2023**. The Paper has been accepted after our double-blind peer review process and plagiarism check.

International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023) will be submitted to the Web of Science Book Citation Index (BkCI) and to SCOPUS for evaluation and indexing.

Authors are recommended to proceed for registration to confirm their slots in relevant scientific sessions by following the link given.

https://icacecsbd.org/conference-registration.php

Introduction to Accepted Paper (Conference Paper) -

The importance of cyber security has become increasingly evident in recent years due to the rise of cyber-attacks and the sophistication of cyber criminals. One of the biggest concerns is application vulnerabilities, which are weaknesses in software that can lead to major issues. As the field of cyber security continues to expand, there is a growing need for skilled security testers and practitioners who can identify and fix vulnerabilities without violating cyber laws. One effective way to learn and test these skills is through intentionally vulnerable web applications, which allow individuals to engage in offensive and defensive operations on their own local system. These web applications simulate real-world web environments and provide a platform for security professionals to practice and enhance their skills in web application security testing, including identifying and fixing technical and non-technical bugs and vulnerabilities. By utilizing these vulnerable web applications, security professionals can better prepare for real-world opportunities and help organizations protect against cyber-attacks.

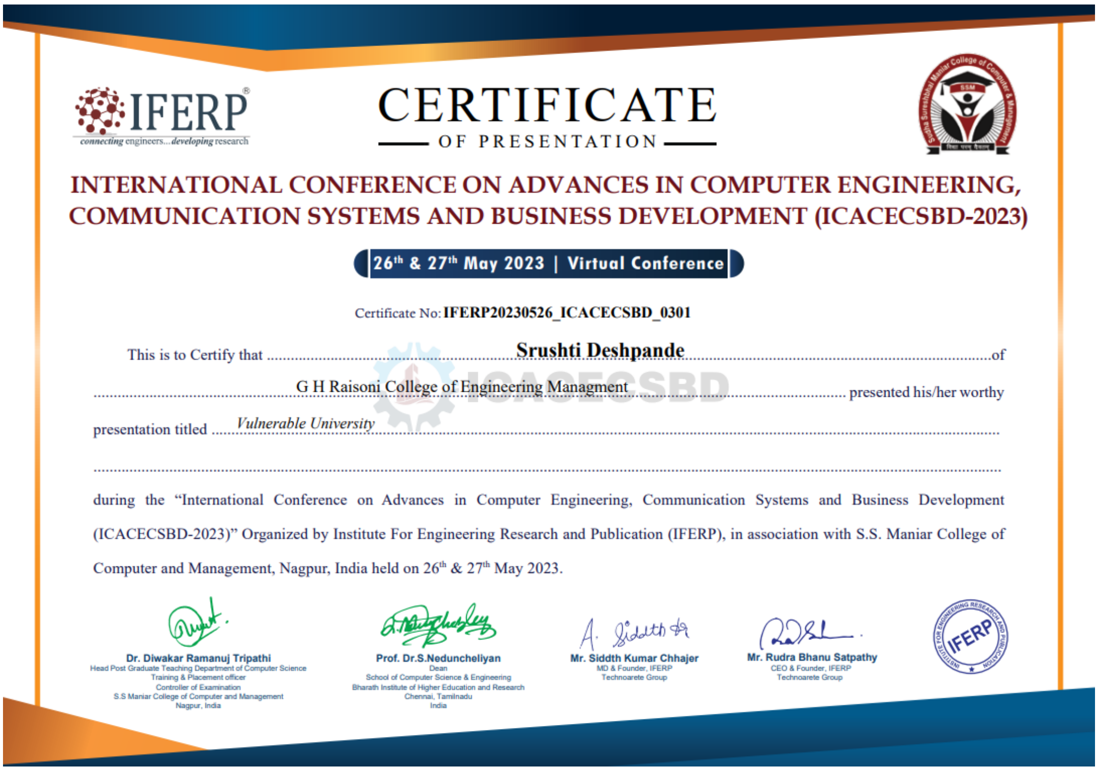
Keywords - Cybersecurity, Vulnerable University, Ethical hacking, Penetration testing, Cyber threats, Cybersecurity professionals, Cybersecurity students, IT security managers, Freelance ethical hackers, Learning and testing, Open-source application, GitHub, Docker file.

Introduction -

The Vulnerable University application is a powerful and effective tool for individuals to learn and practice web application security testing. This intentionally vulnerable web application simulates a university website that contains various vulnerabilities, such as cross-site scripting (XSS), SQL injection, authentication bypass, etc. These vulnerabilities are deliberately included in the application to help users understand and identify security weaknesses in web applications. By navigating through different sections of the website and utilizing various security testing tools and techniques, users can find and exploit these vulnerabilities, and learn how to fix them.

The importance of web application security cannot be overstated in today's digital world, where cyber-attacks are becoming more common and sophisticated. Application vulnerabilities, in particular, pose a significant threat to the security of organizations, making it essential for individuals to have the skills and knowledge to identify and fix these issues. With the Vulnerable University application, developers, security auditors, and penetration testers can practice and enhance their skills in web application security testing in a safe and controlled environment. This enables them to improve their understanding of web application security, identify and fix vulnerabilities, and better prepare themselves for real-world opportunities in the field of cyber security. Overall, the Vulnerable University application is an invaluable resource for anyone looking to learn and develop their skills in web application security testing.

Conference Certificate:



IFERP
connecting engineers...developing research

CERTIFICATE
OF PRESENTATION

INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTER ENGINEERING, COMMUNICATION SYSTEMS AND BUSINESS DEVELOPMENT (ICACECSBD-2023)

26th & 27th May 2023 | Virtual Conference

Certificate No: **IFERP20230526_ICACECSBD_0301**

This is to Certify that **Srushti Deshpande** of G H Raisoni College of Engineering Managment presented his/her worthy presentation titled *Vulnerable University*

during the "International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023)" Organized by Institute For Engineering Research and Publication (IFERP), in association with S.S. Maniar College of Computer and Management, Nagpur, India held on 26th & 27th May 2023.

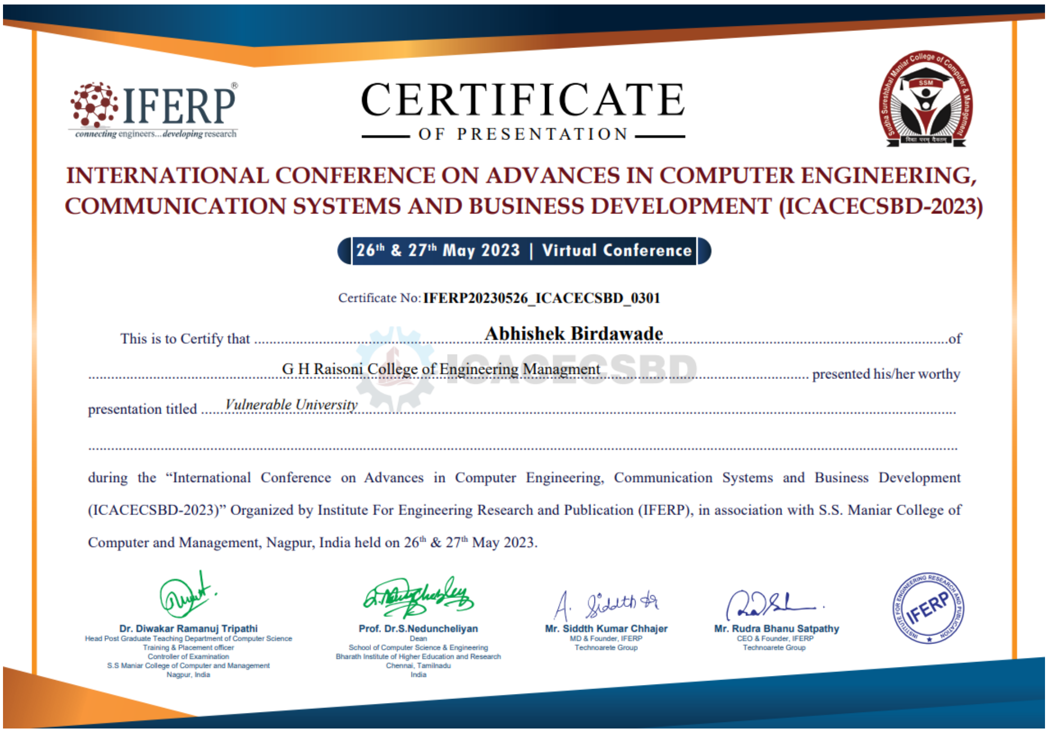
Dr. Diwakar Ramanuj Tripathi
Head Post Graduate Teaching Department of Computer Science
Training & Placement officer
Controller of Examination
S.S Maniar College of Computer and Management
Nagpur, India

Prof. Dr.S.Neduncheliyan
Dean
School of Computer Science & Engineering
Bharath Institute of Higher Education and Research
Chennai, Tamilnadu
India

Mr. Siddth Kumar Chhajer
MD & Founder, IFERP
Technoarete Group

Mr. Rudra Bhanu Satpathy
CEO & Founder, IFERP
Technoarete Group

IFERP
INSTITUTE FOR ENGINEERING RESEARCH AND PUBLICATION



IFERP
connecting engineers... developing research

CERTIFICATE
OF PRESENTATION

INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTER ENGINEERING, COMMUNICATION SYSTEMS AND BUSINESS DEVELOPMENT (ICACECSBD-2023)

26th & 27th May 2023 | Virtual Conference

Certificate No: **IFERP20230526_ICACECSBD_0301**

This is to Certify that **Abhishek Birdawade** of G H Raisoni College of Engineering Managment presented his/her worthy presentation titled *Vulnerable University*

during the "International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023)" Organized by Institute For Engineering Research and Publication (IFERP), in association with S.S. Maniar College of Computer and Management, Nagpur, India held on 26th & 27th May 2023.

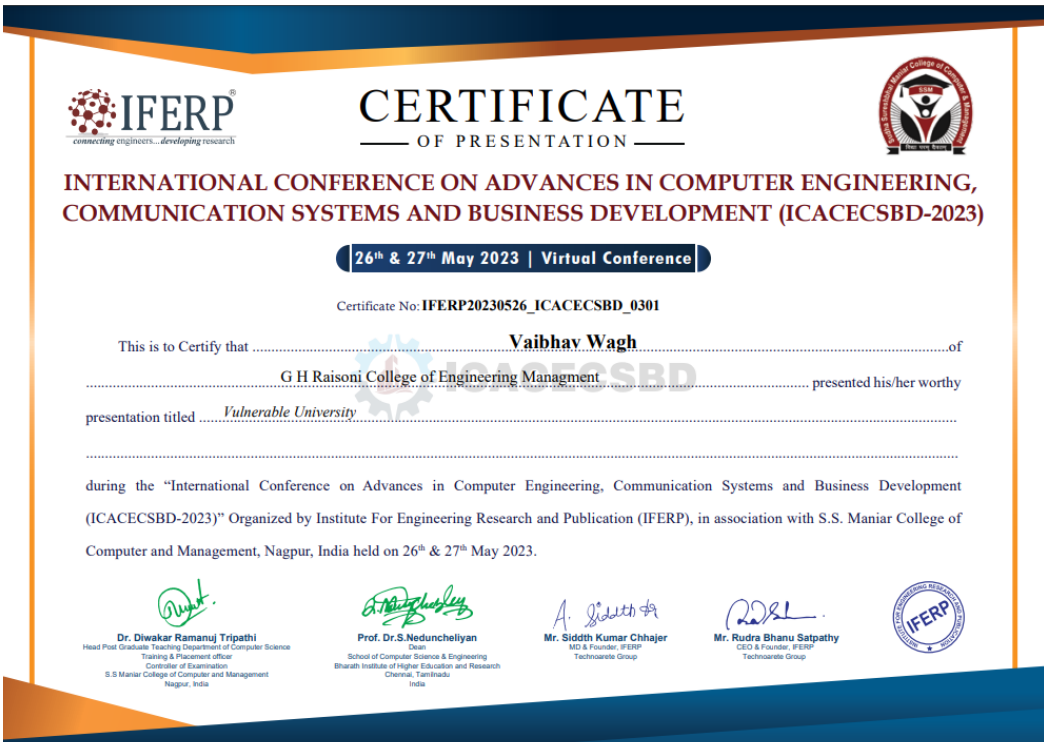
Dr. Diwakar Ramanuj Tripathi
Head Post Graduate Teaching Department of Computer Science
Training & Placement officer
Controller of Examination
S.S Maniar College of Computer and Management
Nagpur, India

Prof. Dr.S.Neduncheliyan
Dean
School of Computer Science & Engineering
Bharath Institute of Higher Education and Research
Chennai, Tamilnadu
India

A. Siddth
Mr. Siddth Kumar Chhajer
MD & Founder, IFERP
Technoarete Group

Mr. Rudra Bhanu Satpathy
CEO & Founder, IFERP
Technoarete Group

INSTITUTE FOR ENGINEERING RESEARCH AND PUBLICATION IFERP



IFERP
connecting engineers... developing research

CERTIFICATE
OF PRESENTATION

INTERNATIONAL CONFERENCE ON ADVANCES IN COMPUTER ENGINEERING, COMMUNICATION SYSTEMS AND BUSINESS DEVELOPMENT (ICACECSBD-2023)

26th & 27th May 2023 | Virtual Conference

Certificate No: **IFERP20230526_ICACECSBD_0301**

This is to Certify that **Vaibhav Wagh** of G H Raisoni College of Engineering Managment presented his/her worthy presentation titled *Vulnerable University*

during the "International Conference on Advances in Computer Engineering, Communication Systems and Business Development (ICACECSBD-2023)" Organized by Institute For Engineering Research and Publication (IFERP), in association with S.S. Maniar College of Computer and Management, Nagpur, India held on 26th & 27th May 2023.

Dr. Diwakar Ramanuj Tripathi
Head Post Graduate Teaching Department of Computer Science
Training & Placement officer
Controller of Examination
S.S Maniar College of Computer and Management
Nagpur, India

Prof. Dr.S.Neduncheliyan
Dean
School of Computer Science & Engineering
Bharath Institute of Higher Education and Research
Chennai, Tamilnadu
India

A. Siddth
Mr. Siddth Kumar Chhajer
MD & Founder, IFERP
Technoarete Group

Mr. Rudra Bhanu Satpathy
CEO & Founder, IFERP
Technoarete Group

INSTITUTE FOR ENGINEERING RESEARCH AND PUBLICATION IFERP

b) Journal Paper

Paper Title: Vulnerable University - Exploring Cybersecurity Vulnerabilities

Name of the Conference/Journal where paper submitted: OpenAIRE

Paper accepted/rejected: Accpeted

Published Date: 23rd May 2023

c) Copyright

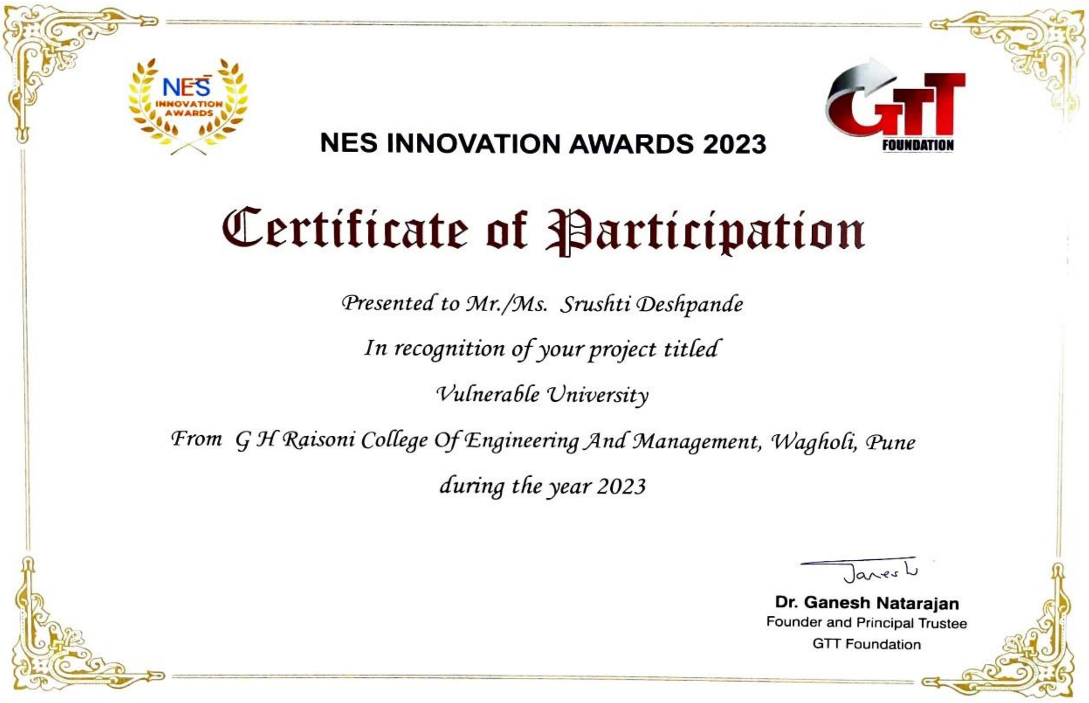
Paper Title: Vulnerable University

Diary Number: 22879/2022-CO/L

Status of Copyright Application: Registered

Appendix D

Participation Certificate



NES INNOVATION AWARDS 2023

Certificate of Participation

Presented to Mr./Ms. Srushti Deshpande

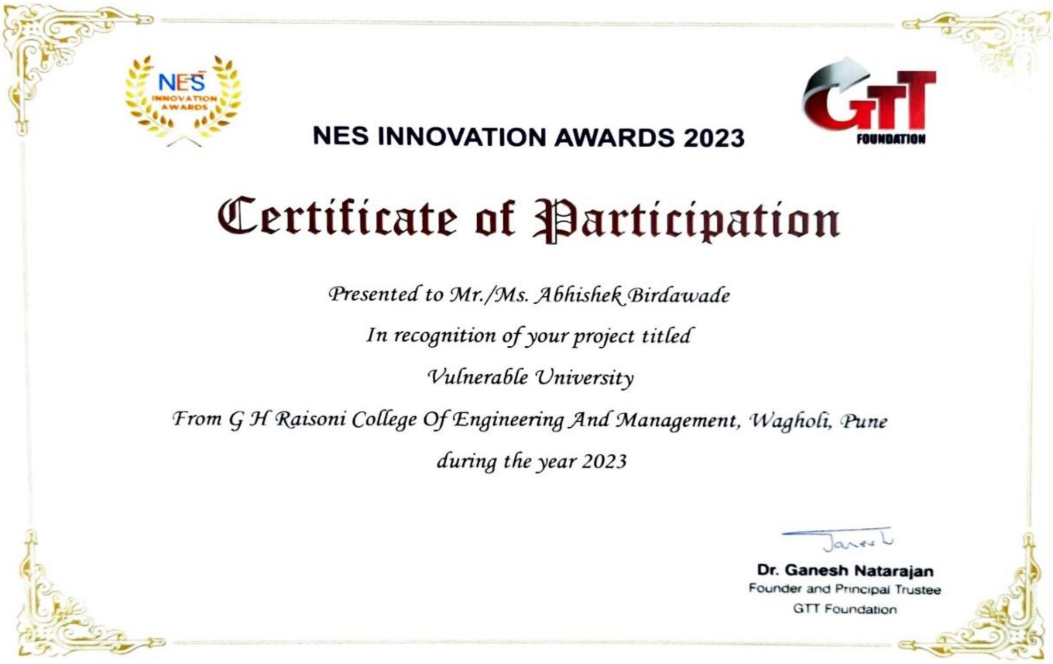
In recognition of your project titled

Vulnerable University

From G H Raisoni College Of Engineering And Management, Wagholi, Pune

during the year 2023

Dr. Ganesh Natarajan
Founder and Principal Trustee
GTT Foundation



NES INNOVATION AWARDS 2023

Certificate of Participation

Presented to Mr./Ms. Abhishek Birdawade

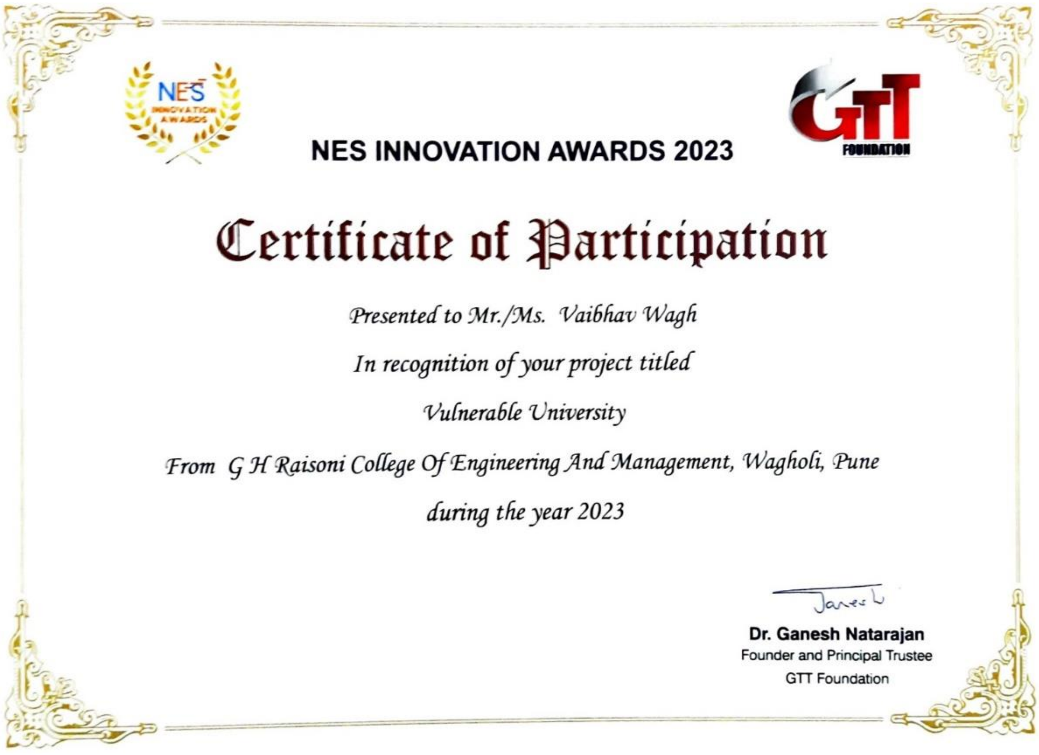
In recognition of your project titled

Vulnerable University

From G H Raisoni College Of Engineering And Management, Wagholi, Pune

during the year 2023

Dr. Ganesh Natarajan
Founder and Principal Trustee
GTT Foundation



NES INNOVATION AWARDS 2023

Certificate of Participation

Presented to Mr./Ms. Vaibhav Wagh

In recognition of your project titled

Vulnerable University

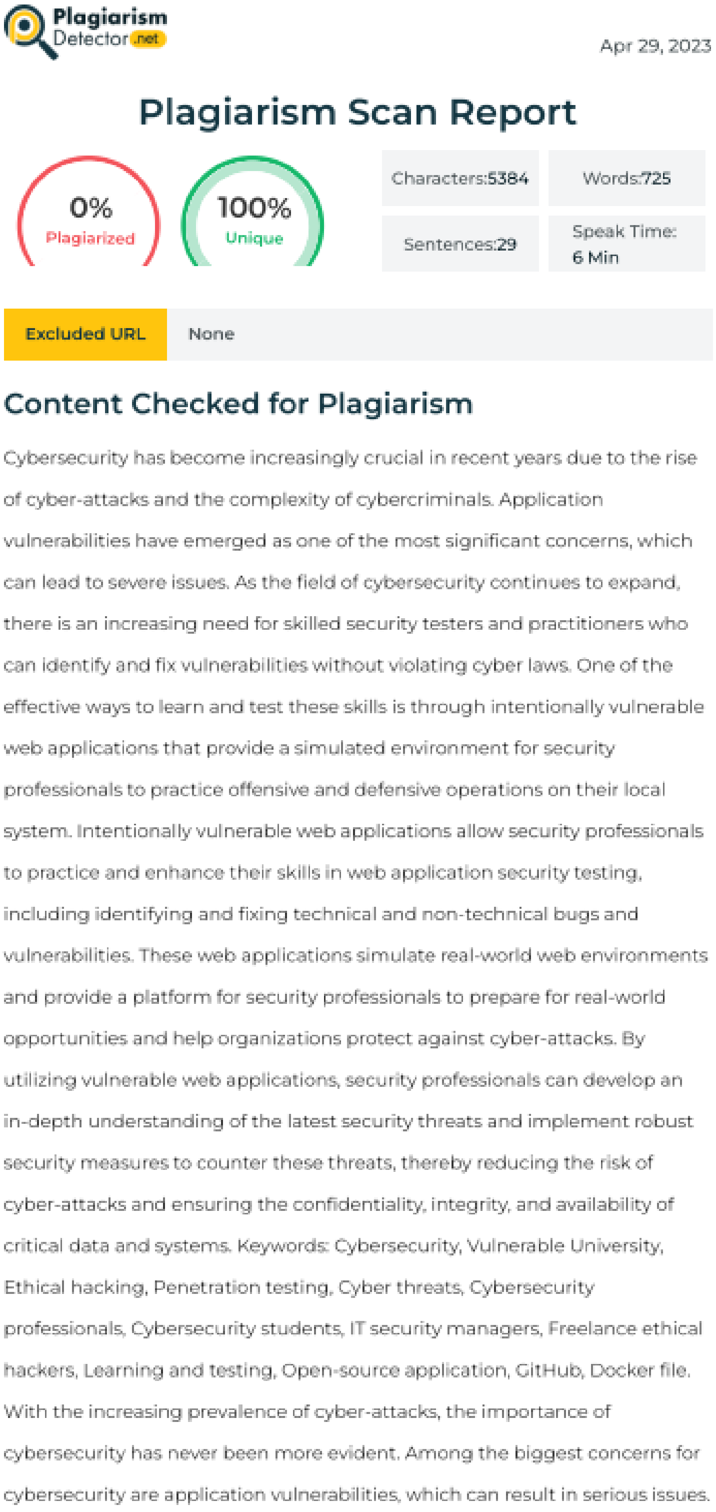
From G H Raisoni College Of Engineering And Management, Wagholi, Pune

during the year 2023

Dr. Ganesh Natarajan
Founder and Principal Trustee
GTT Foundation

Appendix E

Plagiarism Report



Plagiarism Detector .net

Apr 29, 2023

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:5384	Words:725
Sentences:29	Speak Time: 6 Min

Excluded URL	None

Content Checked for Plagiarism

Cybersecurity has become increasingly crucial in recent years due to the rise of cyber-attacks and the complexity of cybercriminals. Application vulnerabilities have emerged as one of the most significant concerns, which can lead to severe issues. As the field of cybersecurity continues to expand, there is an increasing need for skilled security testers and practitioners who can identify and fix vulnerabilities without violating cyber laws. One of the effective ways to learn and test these skills is through intentionally vulnerable web applications that provide a simulated environment for security professionals to practice offensive and defensive operations on their local system. Intentionally vulnerable web applications allow security professionals to practice and enhance their skills in web application security testing, including identifying and fixing technical and non-technical bugs and vulnerabilities. These web applications simulate real-world web environments and provide a platform for security professionals to prepare for real-world opportunities and help organizations protect against cyber-attacks. By utilizing vulnerable web applications, security professionals can develop an in-depth understanding of the latest security threats and implement robust security measures to counter these threats, thereby reducing the risk of cyber-attacks and ensuring the confidentiality, integrity, and availability of critical data and systems. Keywords: Cybersecurity, Vulnerable University, Ethical hacking, Penetration testing, Cyber threats, Cybersecurity professionals, Cybersecurity students, IT security managers, Freelance ethical hackers, Learning and testing, Open-source application, GitHub, Docker file. With the increasing prevalence of cyber-attacks, the importance of cybersecurity has never been more evident. Among the biggest concerns for cybersecurity are application vulnerabilities, which can result in serious issues.

Appendix F

Information of Project Group Members

1 First Member:

- **Name:** Srusthi Deshpande
- **Date of Birth:** 23/10/2001
- **Gender:** Female
- **Permanent Address:** Guruprasad Nagar, Aurangabad, Maharashtra.
- **E-Mail:** srushti.deshpande.cs@ghrcem.raisoni.net
- **Mobile/Contact No.:** 8767306252
- **Placement Details:** Capgemini Technology Services Private Limited

2 Second Member:

- **Name:** Abhishek Birdawade
- **Date of Birth:** 26/05/2001
- **Gender:** Male
- **Permanent Address:** Aaisaheb Nivas, Kelgoan Road, Aalandi Devachi, Pune - 412105
- **E-Mail:** abhishek.birdawade.cs@ghrcem.raisoni.net
- **Mobile/Contact No.:** 7028922734
- **Placement Details:** Appsecco Consultancy – Security Analyst

3 Third Member:

- **Name:** Vaibhav Wagh
- **Date of Birth:** 25/07/2001
- **Gender:** Male
- **Permanent Address:** Type 2A 893 HAL Township Ojhar,Nashik
- **E-Mail:** vaibhav.wagh.cs@ghrcem.raisoni.net
- **Mobile/Contact No.:** 7666286964
- **Placement Details:** Cognizan